UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,838	12/11/2003	Herman Rodriguez	AUS920030905US1(4027)	2206

45557 7590 10/22/2007

IBM CORPORATION (JSS)
C/O SCHUBERT OSTERRIEDER & NICKELSON PLLC
6013 CANNON MOUNTAIN DRIVE, S14
AUSTIN, TX 78749

EXAMINER	
JOHNS, CHRISTOPHER C	
ART UNIT	PAPER NUMBER
4172	

MAIL DATE	DELIVERY MODE
10/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/733,838	RODRIGUEZ ET AL.	
	Examiner	Art Unit	
	Christopher C. Johns	4172	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *14 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/14/05, 12/11/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-8, 10, 11, 14-16, and 18-24 rejected under 35 U.S.C. 102(b) as being anticipated by US Patent Application Publication 2002/0174334 (hereafter referred to as Meadow et al).

As per claim 1:

Meadow et al covers a self-authenticating check system whereby the standard MICR (Magnetic Ink Character Recognition) line includes additional data that includes a one-way hash value. The hash value factors in a private personal identification code from the check writer (***1***: "*providing a purchaser with an encoded personal identification number (PIN)*"). In order to use the information, it must be obtained from the customer (***1***: "*receiving the encoded PIN in response to an offer of payment by the purchaser to a merchant with a check, by a bank associated with the check, wherein the bank is to decode the encoded PIN*") and used with the check to determine whether usage of the check is proper (cf. claim 1) (***1***: "*decoding the encoded PIN, and comparing the decoded PIN with information associated with the purchaser to authenticate the purchaser and to verify that sufficient funds are available to the purchaser for the transaction*").

As per claim 2:

The purchaser must provide the private data to the bank, which will provide it to the check printer (cf. claim 3). Upon receiving the private data, the check printer will generate the MICR data using software (since the data is a one-way hash value, it would be calculated using a computer). While the user does not explicitly have the software to create the MICR, the check printer creates it for him and encrypts it (since it is a one-way hash, cf. claim 1 and paragraphs 8 and 9) (***2***: "*providing the purchaser with software to generate the encoded PIN, wherein generating the encoded PIN comprises encrypting a PIN*").

As per claim 3:

The private data must be communicated to the check printer, because the check printer will print the information on the MICR line "based on information provided from the bank, the information including an n-digit personal code that is not printed on the check" (cf. claim 3). Since the check printer does not have the "n-digit personal code" that is required for the one-way hash, the purchaser must interact with the check printer in order to properly have the encoded data printed on the check (***3***: "*providing the purchaser with the encoded PIN comprises interacting with the purchaser to generate the encoded PIN prior to the transaction*").

As per claim 4:

The merchant will receive the check with the MICR data present on it (claim 1). From there, the MICR and the customer information will be sent to the check verifier for verification. While the Meadow et al system does not send it directly to a bank for processing, the check verifier performs the same service as a bank – verifying the legitimacy of the check transaction (***4***: "*receiving the encoded PIN, forwarded by the merchant to the bank, in an encrypted form such that the merchant is a conduit through which the purchaser transmits to the encoded PIN to the bank*")

As per claim 5:

The Examiner takes Official Notice that the inclusion of transaction information along with any check transaction is inherent to the very definition of a check transaction (***5***: "*receiving the transaction information with the encoded PIN, wherein the transaction information comprises a routing number, a bank account number, a check number, and an amount associated with the transaction.*").

As per claim 6:

The Examiner takes Official Notice that decoding an encrypted piece of data is defined as "decrypting" the data (***6***: "*decoding the encoded PIN comprises decrypting the encoded PIN*").

As per claim 7:

The MICR data contains the check number (cf. paragraph 8), a unique identifier for each check that a purchaser owns and uses (***7***: "*decoding data embedded in the encoded PIN based upon a unique transaction number associated with the purchaser*").

As per claim 8:

The MICR data is known to contain the amount of the transaction (cf., for example, US Patent 4107653, column 2, lines 24-33) (***8***: "*decoding data embedded in the encoded PIN based upon an amount associated with the transaction*").

As per claim 10:

The MICR data in Meadow et al contains a one-way hash. The one-way hash is composed of the check data as well as the "customer-specific information that is not included on the check" (claim 1) e.g.: the private data. This data must be entered correctly so the one-way hash is properly matched. If the one-way hash does not match, the hashes will not match (***10***: "*comparing a password embedded in the decoded PIN against a password received from the purchaser for the transaction*").

As per claim 11:

Meadow et al covers a self-authenticating check system whereby the standard MICR (Magnetic Ink Character Recognition) line includes additional data that includes a one-way hash value. The hash value factors in a private personal identification code from the check writer (***11***: "*PIN module to provide a purchaser with an encoded personal identification number (PIN)*"). In order to use the information, it must be obtained from the customer and used with the check to determine whether usage of the check is proper (cf. claim 1) (***11***: "*a purchaser database to maintain information associated with the purchaser and an account associated with the purchaser, and a PIN processor to receive the encoded PIN in response to an offer of payment by the purchaser to a merchant with a check, decode the encoded PIN, and compare the decoded PIN with the information associated with the purchaser to authenticate the purchaser and to verify that sufficient funds are available to the purchaser for the transaction*").

As per claim 14:

The merchant will receive the check with the MICR data present on it (claim 1). From there, the MICR and the customer information will be sent to the check verifier for verification – without the private customer information, the information on the check cannot be verified. Furthermore, the private customer information is unavailable to the merchant unless explicitly given to him. Furthermore, in one embodiment the data is not given to the merchant at all; rather, the customer enters it on a PIN pad (cf. paragraph 30) (***14***: "*PIN processor is configured to receive the encoded PIN from the merchant, wherein the encoded PIN is designed to prevent the merchant from accessing identification information of the encoded PIN*").

As per claim 15:

The MICR data, containing the one-way hash, must be equal to the one-way hash that is calculated using the account data and the customer private data (cf. paragraph 8 and claim 1) (***15***: "*PIN decrypter to decrypt the encoded PIN*").

As per claim 16:

To read the personal data, the Examiner takes Official Notice that it must be "decoded" (since it is encoded in MICR form) (***16***: "*PIN processor further comprises a PIN decoder to decode the decrypted, encoded PIN*").

As per claim 18:

The MICR data in Meadow et al contains a one-way hash. The one-way hash is composed of the check data as well as the "customer-specific information that is not included on the check" (claim 1) e.g.: the private data. This data must be entered correctly so the one-way hash is properly matched. If the one-way hash does not match, the hashes will not match (***18***: "*comparator is configured to compare a password embedded in the decoded PIN against a password received from the purchaser for the transaction*").

As per claim 19:

Meadow et al covers a self-authenticating check system whereby the standard MICR (Magnetic Ink Character Recognition) line includes additional data that includes a one-way hash value. The hash value factors in a private personal identification code from the check writer (***19***: "*providing a purchaser with an encoded personal identification number (PIN)*"). In order to use the information, it must be obtained from the customer (***19***: "*receiving the encoded PIN in response to an offer of payment by the purchaser to a merchant with a check, by a bank associated with the check, wherein the bank is to decode the encoded PIN*") and used with the check to determine whether usage of the check is proper (cf. claim 1) (***19***: "*decoding the encoded PIN, and comparing the decoded PIN with information associated with the purchaser to authenticate the purchaser and to verify that sufficient funds are available to the purchaser for the transaction*").

As per claim 20:

The purchaser must provide the private data to the bank, which will provide it to the check printer (cf. claim 3). Upon receiving the private data, the check printer will generate the MICR data using software (since the data is a one-way hash value, it would be calculated using a computer). While the user does not explicitly have the software to create the MICR, the check printer creates it for him and encrypts it (since it is a one-way hash, cf. claim 1 and paragraphs 8 and 9) (***20***: "*providing the purchaser with software to generate the encoded PIN*").

As per claim 21:

The private data must be communicated to the check printer, because the check printer will print the information on the MICR line "based on information provided from the bank, the information including an n-digit personal code that is not printed on the check" (cf. claim 3). Since the check printer does not have the "n-digit personal code" that is required for the one-way hash, the purchaser must interact with the check printer in order to properly have the encoded data printed on the check (***21***: "*providing the purchaser with the encoded PIN comprises interacting with the purchaser to encrypt the PIN to generate the encoded PIN prior to the transaction*").

As per claim 22:

The Examiner takes Official Notice that decoding an encrypted piece of data is defined as "decrypting" the data (***22***: "*decoding the encoded PIN comprises decrypting the encoded PIN*").

As per claim 23:

The MICR data contains the check number (cf. paragraph 8), a unique identifier for each check that a purchaser owns and uses (***23***: "*decoding data embedded in the encoded PIN*").

As per claim 24:

The MICR data in Meadow et al contains a one-way hash. The one-way hash is composed of the check data as well as the "customer-specific information that is not included on the check" (claim 1) e.g.: the private data. This data must be entered correctly so the one-way hash is properly matched. If the one-way hash does not match, the hashes will not match (***24***: "*comparing a password embedded in the decoded PIN against a password received from the purchaser for the transaction*").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 9, 12, and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Meadow et al.

As per claim 9:

Using MICR data on checks was well known to those skilled in the art at the time of the invention. Checks also contain the date that the check was written (well known to those skilled in the art at the time of the invention). In the Examiner's best efforts at search, MICR data does not normally contain data pertaining to the date. Including the date in the MICR data would allow for a more full capture of data

As per claim 12:

The purchaser must provide the private data to the bank, which will provide it to the check printer (cf. claim 3). Upon receiving the private data, the check printer will generate the MICR data using software (since the data is a one-way hash value, it would be calculated using a computer). This MICR data depends on both the customer information and the individual check number (cf. paragraph 8). Each check, therefore, will have different information in the MICR data. While the user does not explicitly have the software to create the MICR, the check printer creates it for him and encrypts it (since it is a one-way hash, cf. claim 1 and paragraphs 8 and 9). This could be accomplished by interacting with the purchaser using a software application over the Internet (Examiner takes Official Notice that ordering checks over the Internet was well known to those skilled in the art at the time of the invention). Therefore, it would have been obvious to one skilled in the art at the time of the invention to allow purchasers to use a software application to generate the MICR data based on each individual check (***12***: "*PIN module comprises a client-side software application configured to generate the encoded PIN, the client-side software being configured to independently determine a unique transaction identification that authenticates the purchaser for the transaction to a bank associated with the account*").

As per claim 13:

The purchaser must provide the private data to the bank, which will provide it to the check printer (cf. claim 3). Upon receiving the private data, the check printer will generate the MICR data using software (since the data is a one-way hash value, it would be calculated using a computer). While the user does not explicitly have the software to create the MICR, the check printer creates it for him and encrypts it (since it is a one-way hash, cf. claim 1 and paragraphs 8 and 9). This could be accomplished by interacting with the purchaser using a software application over the Internet (Examiner takes Official Notice that ordering checks over the Internet was well known to those skilled in the art at the time of the invention) (***13***: "*providing the purchaser with software*

to generate the encoded PIN, wherein generating the encoded PIN comprises encrypting a PIN").

Claim 17 rejected under 35 U.S.C. 103(a) as being unpatentable over Meadow et al, in view of US Patent 5,925,865 (hereafter referred to as Steger).

As per claim 17:

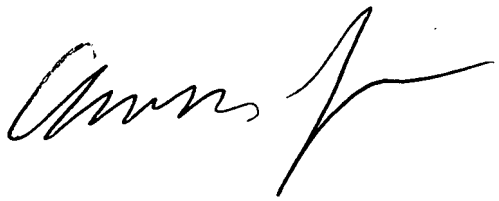
The system in Meadow et al does not explicitly contain a method for verifying the status and amount in an account. However, there is a clear motivation in the checking art for systems that combat fraud. Steger covers a system for "accessing and verifying the status of an account" (column 1, lines 54-55). It also uses a PIN at the point of sale to verify that the check user is a legitimate user. The system "verifies the checking account status and account balance information" (Column 5, lines 52-54) in order to prevent fraud. Both systems (Meadow et al and Steger) aim to prevent fraud through PINs and verification, while Steger adds on account verification to determine if there are funds available for the transaction that is going to take place. There is clear motivation to include this verification in the system in Meadow because of the joint desire to prevent fraud and the ease of implementing it into the system; therefore, it would be obvious to one skilled in the art at the time of the invention to provide for verification services in the system in Meadow et al (***17***: "*PIN processor comprises a comparator to compare the transaction amount with funds available to the purchaser for the transaction.*").

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher C. Johns whose telephone number is 571-270-3462. The examiner can normally be reached on Monday-Thursday, 7:30-5, Alternate Fridays, 7:30-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tom Dixon can be reached on 571-272-6803. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Christopher Johns
Examiner
Art Unit 4172

CCJ

THOMAS A. DIXON
SUPERVISORY PATENT EXAMINER